[Insert Company Logo]

SECURITY AWARENESS & TRAINING GUIDELINES

v1.0

**Instructions:**

* **Use these guidelines to inform everybody who handles any of your company data or access your systems of the awareness training that you will support them in their roles.**
* **Add to, delete from or amend the paragraphs to suit your business requirements.**
* **Publish the document and ensure that everybody who needs it has access and has acknowledged their responsibilities.**

**This document is provided free of charge by CyberSmart Ltd and is to be used as a guide to assist you develop a guidance framework that meets your specific business needs. The document does not constitute or infer any legal advice or guidance.**

# Table of Content

[**Table of Content**](#_4huoebvinxe6) **1**

[**Introduction**](#_3ytswja8z16z) **2**

[**Purpose**](#_tyjcwt) **2**

[**Scope**](#_3dy6vkm) **2**

[**Responsibilities**](#_1t3h5sf) **2**

[**Compliance with legal and contractual obligations**](#_30rduad709pj) **2**

[**On-Boarding Process**](#_4d34og8) **2**

[New employee joining - Compulsory ID Check:](#_75vhumiyzuas) 2

[During the first two week of the new employee joining:](#_rfoyxqg8l176) 2

[**On-Going [add or delete as appropriate to your business]**](#_3rdcrjn) **3**

[**Off-Boarding**](#_lnxbz9) **3**

#

# Introduction

* 1. To protect information it is important that team members, contractors, and other authorised users, who have access to IT systems and equipment understand how their actions affect information security.
	2. Being compliant with IT policies and procedures should result in individuals being made aware of their responsibilities and the consequences of their actions. This will reduce the risk of information loss, leakage or exposure through inadvertent or deliberate actions.

# Purpose

* 1. The purpose of these procedures is to ensure that the security of information and systems is given due importance, it is essential that team members and authorised users:
		1. have the knowledge that policies exist
		2. know where and how to access the policies; and
		3. understood and adhered to policy.

# Scope

* 1. The scope of these procedures includes all team members and contractors.
	2. These procedures apply from on-boarding, ongoing to off-boarding.

# Responsibilities

* 1. [Insert name or appointment] is responsible for clearly communicating the roles and responsibilities to individual team members, team leaders and authorised users.
	2. All employees and contractors are responsible for supporting [insert name or appointment from paragraph 4.1] with information and relevant knowledge to support awareness of and compliance with the guidance.
	3. Team leaders need to be aware that they have a responsibility to ensure that team members have the relevant knowledge concerning information security and systems which they use.
	4. Designated owners of systems, who have responsibility for the management of IT systems and inherent information, need to ensure that team membershave been made aware of their responsibilities toward security.

# Compliance with legal and contractual obligations

* 1. [Insert Company name] is obliged to abide by all UK legislation, it falls upon the individual to be aware of this and also assist in the upholding of this obligation.
	2. To achieve the above, it will be necessary for team membersto be made aware of all policies for the access and use of IT systems and information in general. This will be achieved through a combination of measures such as ongoing training or as part of on-boarding procedures.
	3. Policies should be read, accepted, acknowledged and understood.

# On-Boarding Process

* 1. A record of all security training shall be maintained by [insert name or appointment].

## New employee joining - Compulsory ID Check:

* + 1. Prior to their 1st day of employment all employees must undergo an identity check (international check if foreign national).

## During the first two week of the new employee joining:

* + 1. They must download and synchronise the following software to the existing company accounts:
			1. AV
			2. Anti-malware
			3. Password management
			4. Other software...
		2. In addition, they must ensure the following controls are in place:
			1. Employee machine: Full disk encryption
			2. Employee machine: (macBook) Stealth mode
			3. Employee machine: MDM (if used)
			4. Employee machine: Pin or password protection
			5. Cloud logins: 2FA wherever possible
		3. They have [insert the number sessions] covering all aspects of security.
			1. Typical sessions could cover [add as many as necessary to support your business]:
				1. Reasons why information security is such an important part of the company culture
				2. Signup to any authorised software
				3. Time to read and ask questions on and sign any policies
				4. General security awareness training
				5. Answering any questions, concerns or issues arisen
				6. Ensuring all of the above checks, controls and measures are in place
				7. Accessing and or disclosure of company confidential or restricted information.

# On-Going [add or delete as appropriate to your business]

* 1. We include a rolling agenda slot in our weekly team kick off to communicate any updates about information security and deliver reminders to the team about particular practices.
	2. All team members perform annual security awareness training. Within these sessions all team members are re-familiarised with the policies and processes.
	3. All highly targeted individuals (founders and administrators) perform a higher level of cyber security training in addition to the general security awareness training performed by all team members.
	4. Occasionally social engineering exercises as well as anti-phishing campaigns may be conducted
	5. All team members will only use approved repair centres for repairing and replacement of any assets.
	6. All team members are only allowed to provide their credentials to approved repair centres for the purpose of repair or replacement.
	7. All software provided or recommended must be correctly licenced.

# Off-Boarding

* 1. When a team members contract is terminated, they must return all company assets to CyberSmart.
	2. When a team member’s contract is terminated, individuals shall be denied all access to company information, processes and operations. This includes, but is not limited to company email, [insert any other accesses or software or systems].
	3. When a team member’s or contractor’s contract is terminated, individuals agree to not disclose any company or personal information to anyone not employed by the Company. This includes information regarding the Company’s operational processes and information security system.
	4. All company assets will undergo a factory reset or will be cleansed of all existing information upon return to the Company.

**Signed by**

Name

Appointment

Signature: Date:

**Agreed by**

Name:

Signature: Date: